PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-216766
(43)Date of publication of application : 04.08.2000

(51)Int.Cl. H04L 9/08
G09C 1/00
H04B 7/26
H04Q 7/38

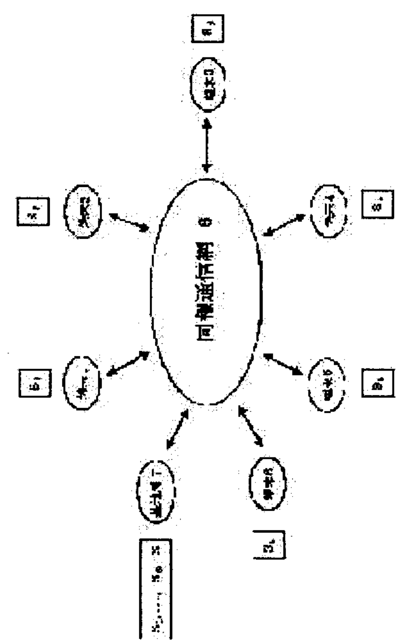
(21)Application number : 11-012227
(22)Date of filing : 20.01.1999

(71)Applicant : KODO IDO TSUSHIN SECURITY GIJUTSU KENKYUSHO:KK
(72)Inventor : ANZAI JUN
MATSUZAKI NATSUME
MATSUMOTO TSUTOMU

(54) EXCLUSIVE KEY SHARING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To accelerate updating of confidential communication by allowing each terminal, capable of being specified by a base station, to hold a secret key and the secret information of a self-terminal calculated from the number of terminals and to find new secret information according to received information, when the base station conducts broadcast communication.

SOLUTION: Each terminal, (i) capable of being specified by a base station, holds a secret key S and a secret information Si satisfying a relational expression defined by a number N of terminals, and the base station holds information including an element (g) of a specified term calculated by the relational expression and secret information S1 to SN. The base station calculates preparation information C1 from the relational expression, calculates elimination information C2 from the secret information Sa of a specific terminal (a), performs broadcast communication of both the number (a) of the terminal (a) and the information C1 to all terminals, finds a shared key K with all of the terminals (i) except the terminal (a), and each terminal (j) finds the key K with the base station by using the information C1 and C2 and own confidential communication Sj. The base station conducts broadcast communication to all of the terminals, finds a new element (g'), replaces it with an element (g), and each terminal (i) finds new confidential communication Si'.



LEGAL STATUS

[Date of request for examination] 02.06.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3032192

[Date of registration] 10.02.2000

[Number of appeal against examiner's decision of

rejection]

[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	10.02.2003

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開2000−216766

（P2000−216766A）

(43)公開日　平成12年8月4日(2000.8.4)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード゛(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ	５Ｋ０６７
Ｈ０４Ｂ　7/26	１０１	Ｈ０４Ｂ　7/26	１０１	
Ｈ０４Ｑ　7/38			１０９Ｓ	
		Ｈ０４Ｌ　9/00	６０１Ｅ	

審査請求　有　　請求項の数８　ＯＬ　（全 21 頁）

(21)出願番号　特願平11−12227

(22)出願日　平成11年１月20日(1999.1.20)

(71)出願人　597174182
株式会社高度移動通信セキュリティ技術研究所
神奈川県横浜市港北区新横浜三丁目20番地8

(72)発明者　安齋　潤
神奈川県横浜市港北区新横浜三丁目20番地8　株式会社高度移動通信セキュリティ技術研究所内

(74)代理人　100099254
弁理士　役　昌明　（外１名）

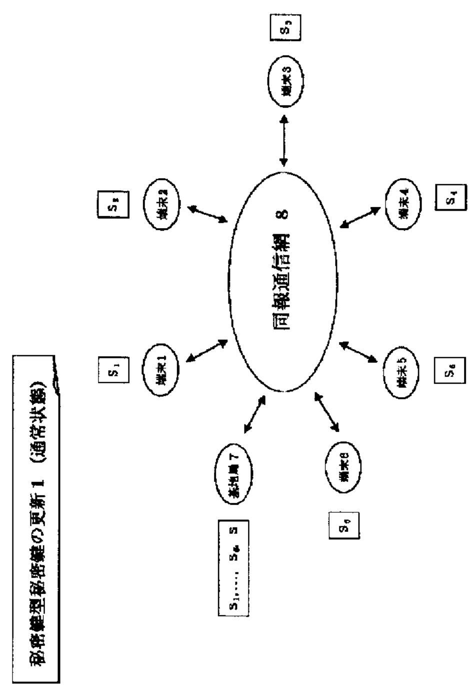
最終頁に続く

(54)【発明の名称】　排他的鍵共有法

(57)【要約】

【課題】　スター型通信システムにおいて、特定の端末を排除するための共通秘密鍵を、少ない通信量で高速に配送する。

【解決手段】　基地局７は秘密鍵Ｓを作成して秘密に保持する。秘密鍵Ｓを分割した秘密情報S_iを、各端末１〜６に暗号通信手段を用いて秘密に配送する。準備情報C_1（$= g^k \bmod p$）と排除情報C_2（$= y_5{}^k \bmod p$）および特定端末番号を全端末に同報通信する。端末は、準備情報C_1と、排除情報C_2を用いて、C_1^(λ(1,Λ) mod q) mod pと、C_2^(λ(5,Λ) mod q) mod pとの積を計算してＫを得て、基地局７との共通データとする。基地局が、零でないＧＦ(q)の元ｅを任意に生成して全端末に同報通信し、新規元ｇ'（$= g^{1/e \bmod q} \bmod p$）を求めて、元ｇと置き換え、各端末ｉが、新規秘密情報S_i'（$= S_i \times e \bmod q$）を求める。基地局の通信量がｅのみと少なく、元ｇ以外の公開情報が変更されないので、高速に秘密情報を更新できる。



【特許請求の範囲】

【請求項１】　基地局と、前記基地局と接続されたＮ台（Ｎは２以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をＳとし、前記Ｓおよび前記Ｎより大きい素数または素数のべき数をｐとし、(ｐ－１)の約数をｑとし、基地局が特定できる端末数（以下、特定端末数という）を１とし、前記各端末ｉ（$1 \leqq i \leqq N$)は、

$S=\sum \lambda(i, \Lambda)\times S_i$（和は$i \in \Lambda$について行う）

（ただし、

$S_i=S+f_1\times i \bmod q$（$f_1$は零でないＧＦ(ｑ)の元）、

$\lambda(i,\Lambda)=\prod \{L/(L-i)\}$（積は$L\in\Lambda-\{i\}$について行う)、

Λは、前記Ｎ台の端末の任意の２台からなる集合である）を満たす秘密情報S_iを秘密に保持しており、前記基地局は、前記（$S, p, g, S_1, \cdots, S_N$）を保持し、（１）前記基地局は、ＧＦ(ｐ)の元をｇとし、零でないＧＦ(ｑ)の元をｋとしたとき、準備情報

$C_1=g^k \bmod p$

を計算し、（２）前記基地局は、特定端末ａの秘密情報S_aから排除情報

$C_2=g\hat{}(k\times S_a \bmod q) \bmod p$

を計算し、特定端末番号ａと準備情報C_1と共に全端末に同報通信し、（３）前記基地局は、前記特定端末ａを除く全ての端末ｊ($j\neq a$)との共有鍵

$K=g\hat{}(k\times S \bmod q) \bmod p$

を求め、（４）前記各端末ｊ($j\neq a$)は、前記準備情報C_1と前記排除情報C_2と自身の秘密情報S_jを用いて、前記S_jと前記$\lambda(j,\Lambda)$の前記法ｑ上での積を指数とする、前記C_1のべき乗剰余値

$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q) \bmod p$

と、前記法ｑ上で求めた前記$\lambda(a,\Lambda)$を指数とする、前記C_2のべき乗剰余値

$C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$

との積

$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$

を計算をすることにより、前記基地局との共有鍵Ｋを求め、（ｉ）前記基地局は、零でないＧＦ(ｑ)の元ｅを任意に生成し、前記ｅを全端末に同報通信し、（ii）前記基地局は、新規元

$g'=g^{1/e \bmod q} \bmod p$

を求め、前記元ｇと置き換え、（iii）前記各端末ｉは、新規秘密情報

$S_i'=S_i\times e \bmod q$

（このとき、$(g')^{Si'} \bmod p=(g)^{Si} \bmod p$が成り立つ）を求めることを特徴とする排他的鍵共有法。

【請求項２】　相互に接続されたＮ台（Ｎは２以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をＳとし、前記Ｓおよび前記Ｎより大きい素数または素数のべき数をｐとし、(ｐ－１)の約数をｑとし、ＧＦ(ｐ)の元をｇとし、議長端末（任意の端末がなることができる）が特定できる特定端末数を１とし、前記各端末ｉ（$1 \leqq i \leqq N$)は、

$S=\sum \lambda(i, \Lambda)\times S_i$（和は$i \in \Lambda$について行う）

（ただし、

$S_i=S+f_1\times i \bmod q$（$f_1$は零でないＧＦ(ｑ)の元）、

$\lambda(i,\Lambda)=\prod \{L/(L-i)\}$（積は$L\in\Lambda-\{i\}$について行う)、

Λは、前記Ｎ台の端末の任意の２台からなる集合である）を満たす秘密情報S_iを秘密に保持しており、システム管理者により管理された前記素数ｐ，前記約数ｑ，前記元ｇと、前記システム管理者により管理された全端末の公開鍵

$y=g^S \bmod p$

と、前記システム管理者により管理された公開情報

$y_1=g^{S1} \bmod p, y_2=g^{S2} \bmod p, \cdots, y_N=g^{SN} \bmod p$

を利用でき、（１）前記議長端末は、零でないＧＦ(ｑ)の元ｋを任意に生成し、準備情報

$C_1=g^k \bmod p$

を計算し、（２）前記議長端末は、特定端末ａの公開情報y_aから排除情報

$C_2={y_a}^k \bmod p$

を計算し、特定端末番号ａと準備情報C_1と共に全端末に同報通信し、（３）前記議長端末は、共有鍵

$K=y^k \bmod p$

を求め、（４）前記各端末ｊ($j\neq a$)は、$\Lambda=\{j,a\}$として、$\lambda(j,\Lambda)$と$\lambda(a,\Lambda)$を求め、前記準備情報C_1と前記排除情報C_2と自身の秘密情報S_jを用いて、

$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$

を計算をすることにより、前記議長端末との共有鍵Ｋを求め、（ｉ）前記システム管理者は、零でないＧＦ(ｑ)の元ｅを任意に生成し、前記ｅを全端末に同報通信し、（ii）前記システム管理者は、新規元

$g'=g^{1/e \bmod q} \bmod p$

を求め、管理する前記元ｇと置き換え、（iii）前記各端末ｉは、新規秘密情報

$S_i'=S_i\times e \bmod q$

（このとき、$(g')^{Si'} \bmod p=(g)^{Si} \bmod p$が成り立つ）を求めることを特徴とする排他的鍵共有法。

【請求項３】　基地局と、前記基地局と接続されたＮ台（Ｎは２以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をＳとし、前記Ｓおよび前記Ｎより大きい素数または素数のべき数をｐとし、(ｐ－１)の約数をｑとし、基地局が特定できる端末数（以下、特定端末数という）を１とし、前記各端末ｉ（$1 \leqq i \leqq N$)は、

$S=\sum\lambda(i,\Lambda)\times S_i$（和は $i\in\Lambda$ について行う）（ただし、$S_i=S+f_1\times i \bmod q$（$f_1$ は零でないGF(q)の元）、$\lambda(i,\Lambda)=\prod\{L/(L-i)\}$（積は $L\in\Lambda-\{i\}$ について行う）、Λ は、前記N台の端末の任意の2台からなる集合である）を満たす秘密情報 S_i を秘密に保持しており、前記基地局は、前記（$S,p,g,S_1,\cdots,S_N$）を保持し、（1）前記基地局は、GF(p)の元をgとし、零でないGF(q)の元をkとしたとき、準備情報

$C_1=g^k \bmod p$

を計算し、（2）前記基地局は、特定端末aの秘密情報 S_a から排除情報

$C_2=g\hat{}(k\times S_a \bmod q) \bmod p$

を計算し、特定端末番号aと準備情報 C_1 と共に全端末に同報通信し、（3）前記基地局は、前記特定端末aを除く全ての端末j（$j\neq a$）との共有鍵

$K=g\hat{}(k\times S \bmod q) \bmod p$

を求め、（4）前記各端末j（$j\neq a$）は、前記準備情報 C_1 と前記排除情報 C_2 と自身の秘密情報 S_j を用いて、前記 S_j と前記 $\lambda(j,\Lambda)$ の前記法q上での積を指数とする、前記 C_1 のべき乗剰余値

$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q) \bmod p$

と、前記法q上で求めた前記 $\lambda(a,\Lambda)$ を指数とする、前記 C_2 のべき乗剰余値

$C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$

との積

$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$

を計算をすることにより、前記基地局との共有鍵Kを求め、（i）前記基地局は、零でないGF(q)の元eを任意に生成し、前記共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、（ii）前記基地局は、新規元

$g'=g^{1/e \bmod q} \bmod p$

を求め、前記元gと置き換え、（iii）前記各端末jは、前記暗号化eを前記共有鍵Kを用いて復号化し、新規秘密情報 $S_j'=S_j\times e \bmod q$

（このとき、$(g')^{Sj'} \bmod p=(g)^{Sj} \bmod p$ が成り立つ）を求めることを特徴とする排他的鍵共有法。

【請求項4】　相互に接続されたN台（Nは2以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、（p−1）の約数をqとし、GF(p)の元をgとし、議長端末（任意の端末がなることができる）が特定できる特定端末数を1とし、前記各端末i（$1\leq i\leq N$）は、

$S=\sum\lambda(i,\Lambda)\times S_i$（和は $i\in\Lambda$ について行う）（ただし、$S_i=S+f_1\times i \bmod q$（$f_1$ は零でないGF(q)の元）、$\lambda(i,\Lambda)=\prod\{L/(L-i)\}$（積は $L\in\Lambda-\{i\}$ について行う）、Λ は、前記N台の端末の任意の2台からなる集合である）を満たす秘密情報 S_i を秘密に保持しており、全端末の公開鍵

$y=g^S \bmod p$

と、公開情報

$y_1=g^{S1} \bmod p, y_2=g^{S2} \bmod p,\cdots, y_N=g^{SN} \bmod p$

を利用でき、（1）前記議長端末は、零でないGF(q)の元kを任意に生成し、準備情報

$C_1=g^k \bmod p$

を計算し、（2）前記議長端末は、特定端末aの公開情報 y_a から排除情報

$C_2=y_a{}^k \bmod p$

を計算し、特定端末番号aと準備情報 C_1 と共に全端末に同報通信し、（3）前記議長端末は、共有鍵

$K=y^k \bmod p$

を求め、（4）前記各端末j（$j\neq a$）は、$\Lambda=\{j,a\}$ として、$\lambda(j,\Lambda)$ と $\lambda(a,\Lambda)$ を求め、前記準備情報 C_1 と前記排除情報 C_2 と自身の秘密情報 S_j を用いて、

$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$

を計算をすることにより、前記議長端末との共有鍵Kを求め、（i）前記議長端末は、零でないGF(q)の元eを任意に生成し、前記共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、（ii）前記議長端末は、新規元

$g'=g^{1/e \bmod q} \bmod p$

を求め、前記元gと置き換え、（iii）前記各端末jは、前記暗号化eを前記共有鍵Kを用いて復号化し、新規秘密情報

$S_j'=S_j\times e \bmod q$

（このとき、$(g')^{Sj'} \bmod p=(g)^{Sj} \bmod p$ が成り立つ）を求めることを特徴とする排他的鍵共有法。

【請求項5】　相互に接続されたN台（Nは2以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、（p−1）の約数をqとし、GF(p)の元をgとし、議長端末bが特定できる特定端末数を1とし、前記各端末i（$1\leq i\leq N$）は、

$S=\sum\lambda(i,\Lambda)\times S_i$（和は $i\in\Lambda$ について行う）（ただし、$S_i=S+f_1\times i \bmod q$（$f_1$ は零でないGF(q)の元）、$\lambda(i,\Lambda)=\prod\{L/(L-i)\}$（積は $L\in\Lambda-\{i\}$ について行う）、Λ は、前記N台の端末の任意の2台からなる集合である）を満たす秘密情報 S_i を秘密に保持しており、前記

議長端末bは、全端末の公開鍵

$y=g^S \bmod p$

と、公開情報

$y_1=g^{S1} \bmod p, y_2=g^{S2} \bmod p, \cdots, y_N=g^{SN} \bmod p$

を利用でき、(1)前記議長端末bは、零でないGF(q)の元kを任意に生成し、準備情報

$C_1=g^k \bmod p$

を計算し、(2)前記議長端末bは、特定端末aの公開情報y_aから排除情報

$C_2=y_a{}^k \bmod p$

を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信し、(3)前記議長端末bは、共有鍵

$K=y^k \bmod p$

を求め、(4)前記各端末j(j≠a,b)は、Λ={j,a}として、λ(j,Λ)とλ(a,Λ)を求め、前記準備情報C_1と前記排除情報C_2と自身の秘密情報S_jを用いて、

C_1^(S_j×λ(j,Λ) mod q)×C_2^(λ(a,Λ) mod q) mod p

を計算をすることにより、共有鍵Kを求めることを特徴とする排他的鍵共有法。

【請求項6】　前記議長端末bを除く全ての端末は、前記議長端末bの公開情報

$y_b=g^{Sb} \bmod p$

を利用でき、前記議長端末bが、前記議長端末bの秘密情報S_bを用いて、全端末に配送する特定端末番号aと準備情報C_1と排除情報C_2に、ディジタル署名を付加し、前記各端末jが、前記議長端末の公開情報y_bを用いて、署名の検証を行うことを特徴とする請求項5記載の排他的鍵共有法。

【請求項7】　上記基地局または議長端末が、上記特定端末aに対して、上記元eを配送し、上記特定端末aは、新規秘密情報

$S_a{}'=S_a \times e \bmod q$

(このとき、(g')^S_a' mod p=(g)^S_a mod pが成り立つ)を求めることを特徴とする請求項3、4記載の排他的鍵共有法。

【請求項8】　前記乗法演算を、任意の有限体上の楕円曲線などの曲線上の加法演算に対応させることを特徴とする請求項1～7記載の排他的鍵共有法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、基地局と複数端末からなるスター型通信システムなどにおける暗号鍵共有方法に関し、特に、基地局が特定した端末以外のすべての端末に共通の秘密鍵を安全に配送する鍵共有方法、および特定の端末のみに共有の秘密鍵を安全に配送する鍵共有方法に関する。

【0002】

【従来の技術】基地局が複数の端末を管理するスター型通信システムにおいて、基地局と傘下の複数の端末がグループを形成し、グループで同じグループ秘密鍵を共有して同報の暗号通信を行う場合がある。この場合、グループ秘密鍵を用いて暗号化された情報は、同じ秘密鍵を保有するグループ内の端末だけが復号することができる。

【0003】ところで、このグループから特定の端末を排除したい場合が生じる。それは、例えば、グループ内のある端末が盗難にあい、その端末を用いた暗号通信の盗聴や偽情報の送信などの不正が行われるおそれがある場合などである。このとき、この秘密鍵を管理する基地局は、できるだけ速やかに、盗難にあった端末を排除してグループ秘密鍵を更新し、残りの端末だけで新たな秘密鍵を共有することが必要となる。

【0004】また、新たにグループを構成する必要が生じる場合がある。それは、グループ外の端末をグループに加入させる場合や、別のグループの端末を一つのグループにする場合などである。このとき、基地局は、できるだけ速やかに、新規グループの鍵をグループを構成する端末と共有することが必要となる。

【0005】このような目的を達成するため、本発明者は先に、以下のような効率的な排他的鍵共有法を提案した。

【0006】基地局と、基地局と接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムにおいて、秘密鍵をSとし、SおよびNより大きい素数または素数のべき数をpとし、(p−1)の約数をqとし、基地局が特定できる端末数(以下、特定端末数という)を1とし、各端末i(1≦i≦N)は、

S=Σλ(i,Λ)×S_i(和はi∈Λについて行う)

(ただし、

$S_i=S+f_1 \times i \bmod q$($f_1$は零でないGF(q)の元)

λ(i,Λ)=Π{L/(L−i)}(積はL∈Λ−{i}について行う)

Λは、N台の端末の任意の2台からなる集合)を満たす秘密情報S_iを秘密に保持しており、基地局は、(S,p,g,S_1,…,S_N)を保持している。

(1)基地局は、GF(p)の元をgとし、零でないGF(q)の元をkとしたとき、準備情報

$C_1=g^k \bmod p$

を計算する。

(2)基地局は、特定端末aの秘密情報S_aから排除情報

C_2=g^(k×S_a mod q) mod p

を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信する。

(3)基地局は、特定端末aを除く全ての端末j(j≠a)との共有鍵

K=g^(k×S mod q) mod p

を求める。

（4）各端末j（$j \neq a$）は、準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、S_jと$\lambda(j, \Lambda)$の法q上での積を指数とする、C_1のべき乗剰余値

C_1^$(S_j \times \lambda(j, \Lambda) \bmod q) \bmod p$

と、法q上で求めた$\lambda(a, \Lambda)$を指数とする、C_2のべき乗剰余値

C_2^$(\lambda(a, \Lambda) \bmod q) \bmod p$

との積

C_1^$(S_j \times \lambda(j, \Lambda) \bmod q) \times C_2$^$(\lambda(a, \Lambda) \bmod q) \bmod p$

を計算をすることにより、基地局との共有鍵Kを求める。

【0007】このようにして、基地局から全端末に同報通信をするだけで鍵共有ができるので、鍵共有のための業務停止期間を短くできるとともに、端末での処理が削減できるので、計算能力が高くない端末で高速に鍵共有ができる。

【0008】

【発明が解決しようとする課題】しかし、上記の鍵共有方法では、次の3つの問題が存在する。

（1）安全性を高めるために端末の秘密情報を定期的に更新するのが望ましいが、各端末毎に新規秘密情報を配送すると、通信量と更新が終了するまでの時間が多くなっていた。また、一般に秘密情報を更新すると公開情報の更新が必要となり、公開簿や端末がローカルに保存している公開情報の更新も行うので更新時間が多くなっていた。

（2）前回の排他的鍵共有で排除した端末を、それ以降の全ての排他的鍵共有でも排除し続けるためには、排他的鍵共有毎に処理を必要としていた。

（3）端末のみからなるシステムにおいて排他的鍵共有を行うには、全端末が他の全端末の公開情報を保有しているか、それらが公開された公開簿が必要であった。また、誰でもが議長端末になれる方法であるので、運用上議長端末をある端末に固定したい場合に対応できなかった。

【0009】本発明は、上記の課題を解決して、通信量と更新時間を最小に押さえて全端末の秘密情報を更新すること、排他的鍵共有毎に処理を行うことなく1度排除した端末を継続的に排除すること、各端末が全端末の公開情報を保有せず、かつ公開簿を必要ないようにすること、ある端末だけが議長端末になれるようにすることを目的とする。

【0010】

【課題を解決するための手段】上記の課題を解決するために、本発明では、基地局と、基地局と接続されたN台（Nは2以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法を、秘密鍵をSとし、SおよびNより大きい素数または素数のべき数をpとし、$(p-1)$の約数をqとし、基地局が特定できる端末数（以下、特定端末数という）を1とし、各端末i（$1 \leq i \leq N$）は、

$S = \sum \lambda(i, \Lambda) \times S_i$（和は$i \in \Lambda$について行う）

（ただし、

$S_i = S + f_1 \times i \bmod q$（$f_1$は零でないGF(q)の元）、

$\lambda(i, \Lambda) = \prod \{L/(L-i)\}$（積は$L \in \Lambda - \{i\}$について行う）、

Λは、N台の端末の任意の2台からなる集合である）を満たす秘密情報S_iを秘密に保持しており、基地局は、$(S, p, g, S_1, \cdots, S_N)$を保持し、（1）基地局は、GF(p)の元をgとし、零でないGF(q)の元をkとしたとき、準備情報

$C_1 = g^k \bmod p$

を計算し、（2）基地局は、特定端末aの秘密情報S_aから排除情報

$C_2 = g$^$(k \times S_a \bmod q) \bmod p$

を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信し、（3）基地局は、特定端末aを除く全ての端末j（$j \neq a$）との共有鍵

$K = g$^$(k \times S \bmod q) \bmod p$

を求め、（4）各端末j（$j \neq a$）は、準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、S_jと$\lambda(j, \Lambda)$の法q上での積を指数とする、C_1のべき乗剰余値

C_1^$(S_j \times \lambda(j, \Lambda) \bmod q) \bmod p$

と、法q上で求めた$\lambda(a, \Lambda)$を指数とする、C_2のべき乗剰余値

C_2^$(\lambda(a, \Lambda) \bmod q) \bmod p$

との積

C_1^$(S_j \times \lambda(j, \Lambda) \bmod q) \times C_2$^$(\lambda(a, \Lambda) \bmod q) \bmod p$

を計算をすることにより、基地局との共有鍵Kを求め、（i）基地局は、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、（ii）基地局は、新規元

$g' = g^{1/e \bmod q} \bmod p$

を求め、元gと置き換え、（iii）各端末iは、新規秘密情報

$S_i' = S_i \times e \bmod q$

（このとき、$(g')^{S_i'} \bmod p = (g)^{S_i} \bmod p$が成り立つ）を求める構成とした。

【0011】このように構成したことにより、基地局の通信量がeのみと少なく、システムパラメータ元g以外の公開情報が変更されないので、高速な秘密情報の更新が可能となる。

【0012】また、互に接続されたN台（Nは2以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、（i）システム管理者は、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、（ii）システム管理者は、新規元

$g' = g^{1/e \bmod q} \bmod p$

を求め、管理する元gと置き換え、(iii) 各端末iは、新規秘密情報

$S_i' = S_i \times e \bmod q$

を求める構成とした。

【0013】このように構成したことにより、システム管理者の通信量がeのみと少なく、システムパラメータ元g以外の公開情報が変更されないので、高速な秘密情報の更新が可能となる。

【0014】また、基地局と、基地局と接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i) 基地局は、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、(ii) 基地局は、新規元

$g' = g^{1/e \bmod q} \bmod p$

を求め、元gと置き換え、(iii) 各端末jは、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報

$S_j' = S_j \times e \bmod q$

を求める構成とした。

【0015】このように構成したことにより、排他的鍵共有で共有した共有鍵を用いて配送した乱数を用いて端末の秘密情報を更新するので、以降の排他的鍵共有で排除した端末は復帰することができない。

【0016】また、相互に接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i) 議長端末は、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、(ii) 議長端末は、新規元

$g' = g^{1/e \bmod q} \bmod p$

を求め、元gと置き換え、(iii) 各端末jは、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報

$S_j' = S_j \times e \bmod q$

を求める構成とした。

【0017】このように構成したことにより、排他的鍵共有で共有した共有鍵を用いて配送した乱数を用いて端末の秘密情報を更新するので、以降の排他的鍵共有で排除した端末は復帰することができない。

【0018】また、相互に接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、SおよびNより大きい素数または素数のべき数をpとし、(p−1)の約数をqとし、GF(p)の元をgとし、議長端末bが特定できる特定端末数を1とし、各端末i(1≦i≦N)は、

$S = \sum \lambda(i, \Lambda) \times S_i$ (和は$i \in \Lambda$について行う)

(ただし、

$S_i = S + f_1 \times i \bmod q$ (f_1は零でないGF(q)の元)、

$\lambda(i, \Lambda) = \prod \{L/(L-i)\}$ (積は$L \in \Lambda - \{i\}$について行う)、

Λは、N台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持しており、議長端末bは、全端末の公開鍵

$y = g^S \bmod p$

と、公開情報

$y_1 = g^{S1} \bmod p, y_2 = g^{S2} \bmod p, \cdots, y_N = g^{SN} \bmod p$

を利用でき、(1) 議長端末bは、零でないGF(q)の元kを任意に生成し、準備情報

$C_1 = g^k \bmod p$

を計算し、(2) 議長端末bは、特定端末aの公開情報y_aから排除情報

$C_2 = y_a{}^k \bmod p$

を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信し、(3) 議長端末bは、共有鍵

$K = y^k \bmod p$

を求め、(4) 各端末j ($j \neq a, b$)は、$\Lambda = \{j, a\}$として、$\lambda(j, \Lambda)$と$\lambda(a, \Lambda)$を求め、準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、

$C_1\hat{}(S_j \times \lambda(j, \Lambda) \bmod q) \times C_2\hat{}(\lambda(a, \Lambda) \bmod q) \bmod p$

を計算をすることにより、共有鍵Kを求める構成とした。

【0019】このように構成したことにより、議長端末以外の端末は他の端末の公開情報を保持する必要が無く、議長端末のみが他の端末の公開情報を利用できるので他の端末は議長端末になれない。

【0020】

【発明の実施の形態】本発明の請求項1記載の発明は、基地局と、前記基地局と接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、前記Sおよび前記Nより大きい素数または素数のべき数をpとし、(p−1)の約数をqとし、基地局が特定できる端末数(以下、特定端末数という)を1とし、前記各端末i(1≦i≦N)は、

$S = \sum \lambda(i, \Lambda) \times S_i$ (和は$i \in \Lambda$について行う)

(ただし、

$S_i = S + f_1 \times i \bmod q$ (f_1は零でないGF(q)の元)、

$\lambda(i, \Lambda) = \prod \{L/(L-i)\}$ (積は$L \in \Lambda - \{i\}$について行う)、

Λは、前記N台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持しており、前記基地局は、前記$(S, p, g, S_1, \cdots, S_N)$を保持し、(1) 前記基地局は、GF(p)の元をgとし、零でないGF(q)の元をkとしたとき、準備情報

$C_1 = g^k \bmod p$

を計算し、(2) 前記基地局は、特定端末aの秘密情報

S_aから排除情報

$C_2=g$^$(k\times S_a \bmod q) \bmod p$

を計算し、特定端末番号ａと準備情報C_1と共に全端末に同報通信し、（３）前記基地局は、前記特定端末ａを除く全ての端末ｊ（$j\neq a$）との共有鍵

$K=g$^$(k\times S \bmod q) \bmod p$

を求め、（４）前記各端末ｊ（$j\neq a$）は、前記準備情報C_1と前記排除情報C_2と自身の秘密情報S_jを用いて、前記S_jと前記$\lambda(j,\Lambda)$の前記法ｑ上での積を指数とする、前記C_1のべき乗剰余値

C_1^$(S_j\times\lambda(j,\Lambda) \bmod q) \bmod p$

と、前記法ｑ上で求めた前記$\lambda(a,\Lambda)$を指数とする、前記C_2のべき乗剰余値

C_2^$(\lambda(a,\Lambda) \bmod q) \bmod p$

との積

C_1^$(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2$^$(\lambda(a,\Lambda) \bmod q) \bmod p$

を計算をすることにより、前記基地局との共有鍵Ｋを求め、（ｉ）前記基地局は、零でないＧＦ（ｑ）の元ｅを任意に生成し、前記ｅを全端末に同報通信し、（ii）前記基地局は、新規元

$g'=g^{1/e \bmod q} \bmod p$

を求め、前記元ｇと置き換え、（iii）前記各端末ｉは、新規秘密情報

$S_i'=S_i\times e \bmod q$

（このとき、$(g')^{Si'} \bmod p=(g)^{Si} \bmod p$が成り立つ）を求める排他的鍵共有法であり、基地局からのｅのみの配送により少ない通信量で安全に端末秘密鍵の更新を行うという作用を有する。

【００２１】本発明の請求項２記載の発明は、相互に接続されたN台（Nは2以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をＳとし、前記Ｓおよび前記Ｎより大きい素数または素数のべき数をｐとし、(ｐ－１)の約数をｑとし、ＧＦ(ｐ)の元をｇとし、議長端末（任意の端末がなることができる）が特定できる特定端末数を１とし、前記各端末ｉ（$1\leqq i\leqq N$)は、

$S=\sum\lambda(i,\Lambda)\times S_i$（和は$i\in\Lambda$について行う）

（ただし、

$S_i=S+f_1\times i \bmod q$（$f_1$は零でないＧＦ(ｑ)の元）、

$\lambda(i,\Lambda)=\prod\{L/(L-i)\}$（積は$L\in\Lambda-\{i\}$について行う）、

Λは、前記Ｎ台の端末の任意の２台からなる集合である）を満たす秘密情報S_iを秘密に保持しており、システム管理者により管理された前記素数ｐ，前記約数ｑ，前記元ｇと、前記システム管理者により管理された全端末の公開鍵

$y=g^S \bmod p$

と、前記システム管理者により管理された公開情報

$y_1=g^{S1} \bmod p, y_2=g^{S2} \bmod p,\cdots, y_N=g^{SN} \bmod p$

を利用でき、（１）前記議長端末は、零でないＧＦ(ｑ)の元ｋを任意に生成し、準備情報

$C_1=g^k \bmod p$

を計算し、（２）前記議長端末は、特定端末ａの公開情報y_aから排除情報

$C_2={y_a}^k \bmod p$

を計算し、特定端末番号ａと準備情報C_1と共に全端末に同報通信し、（３）前記議長端末は、共有鍵

$K=y^k \bmod p$

を求め、（４）前記各端末ｊ（$j\neq a$）は、$\Lambda=\{j,a\}$として、$\lambda(j,\Lambda)$と$\lambda(a,\Lambda)$を求め、前記準備情報C_1と前記排除情報C_2と自身の秘密情報S_jを用いて、

C_1^$(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2$^$(\lambda(a,\Lambda) \bmod q) \bmod p$

を計算をすることにより、前記議長端末との共有鍵Ｋを求め、（ｉ）前記システム管理者は、零でないＧＦ（ｑ）の元ｅを任意に生成し、前記ｅを全端末に同報通信し、（ii）前記システム管理者は、新規元

$g'=g^{1/e \bmod q} \bmod p$

を求め、管理する前記元ｇと置き換え、（iii）前記各端末ｉは、新規秘密情報

$S_i'=S_i\times e \bmod q$

（このとき、$(g')^{Si'} \bmod p=(g)^{Si} \bmod p$が成り立つ）を求める排他的鍵共有法であり、システム管理者によるｅのみの少ない通信量の端末秘密鍵の配送で公開鍵暗号の秘密鍵を安全高速に更新するという作用を有する。

【００２２】本発明の請求項３記載の発明は、基地局と、前記基地局と接続されたＮ台（Ｎは２以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をＳとし、前記Ｓおよび前記Ｎより大きい素数または素数のべき数をｐとし、(ｐ－１)の約数をｑとし、基地局が特定できる端末数（以下、特定端末数という）を１とし、前記各端末ｉ（$1\leqq i\leqq N$)は、

$S=\sum\lambda(i,\Lambda)\times S_i$（和は$i\in\Lambda$について行う）

（ただし、

$S_i=S+f_1\times i \bmod q$（$f_1$は零でないＧＦ(ｑ)の元）、

$\lambda(i,\Lambda)=\prod\{L/(L-i)\}$（積は$L\in\Lambda-\{i\}$について行う）、

Λは、前記Ｎ台の端末の任意の２台からなる集合である）を満たす秘密情報S_iを秘密に保持しており、前記基地局は、前記（$S,p,g,S_1,\cdots,S_N$）を保持し、（１）前記基地局は、ＧＦ(ｐ)の元をｇとし、零でないＧＦ(ｑ)の元をｋとしたとき、準備情報

$C_1=g^k \bmod p$

を計算し、（２）前記基地局は、特定端末ａの秘密情報S_aから排除情報

$C_2=g$^$(k\times S_a \bmod q) \bmod p$

を計算し、特定端末番号ａと準備情報C_1と共に全端末に同報通信し、（３）前記基地局は、前記特定端末ａを除く全ての端末ｊ（$j \neq a$）との共有鍵

$K = g\hat{}(k \times S \bmod q) \bmod p$

を求め、（４）前記各端末ｊ（$j \neq a$）は、前記準備情報C_1と前記排除情報C_2と自身の秘密情報S_jを用いて、前記S_jと前記$\lambda(j, \Lambda)$の前記法ｑ上での積を指数とする、前記C_1のべき乗剰余値

$C_1\hat{}(S_j \times \lambda(j, \Lambda) \bmod q) \bmod p$

と、前記法ｑ上で求めた前記$\lambda(a, \Lambda)$を指数とする、前記C_2のべき乗剰余値

$C_2\hat{}(\lambda(a, \Lambda) \bmod q) \bmod p$

との積

$C_1\hat{}(S_j \times \lambda(j, \Lambda) \bmod q) \times C_2\hat{}(\lambda(a, \Lambda) \bmod q) \bmod p$

を計算をすることにより、前記基地局との共有鍵Ｋを求め、（ｉ）前記基地局は、零でないＧＦ（ｑ）の元ｅを任意に生成し、前記共有鍵Ｋを用いて暗号化した暗号化ｅを全端末に同報通信し、（ii）前記基地局は、新規元

$g' = g^{1/e \bmod q} \bmod p$

を求め、前記元ｇと置き換え、（iii）前記各端末ｊは、前記暗号化ｅを前記共有鍵Ｋを用いて復号化し、新規秘密情報

$S_j' = S_j \times e \bmod q$

（このとき、$(g')^{Sj'} \bmod p = (g)^{Sj} \bmod p$が成り立つ）を求める排他的鍵共有法であり、基地局により秘密鍵を更新して排除端末を継続的に排除するという作用を有する。

【００２３】本発明の請求項４記載の発明は、相互に接続されたＮ台（Ｎは２以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をＳとし、前記Ｓおよび前記Ｎより大きい素数または素数のべき数をｐとし、（ｐ－１）の約数をｑとし、ＧＦ（ｐ）の元をｇとし、議長端末（任意の端末がなることができる）が特定できる特定端末数を１とし、前記各端末ｉ（$1 \leqq i \leqq N$）は、

$S = \sum \lambda(i, \Lambda) \times S_i$（和は$i \in \Lambda$について行う）

（ただし、

$S_i = S + f_1 \times i \bmod q$（$f_1$は零でないＧＦ（ｑ）の元）、

$\lambda(i, \Lambda) = \prod \{L / (L - i)\}$（積は$L \in \Lambda - \{i\}$について行う）、

Λは、前記Ｎ台の端末の任意の２台からなる集合である）を満たす秘密情報S_iを秘密に保持しており、全端末の公開鍵

$y = g^S \bmod p$

と、公開情報

$y_1 = g^{S1} \bmod p, y_2 = g^{S2} \bmod p, \cdots, y_N = g^{SN} \bmod p$

を利用でき、（１）前記議長端末は、零でないＧＦ（ｑ）の元ｋを任意に生成し、準備情報

$C_1 = g^k \bmod p$

を計算し、（２）前記議長端末は、特定端末ａの公開情報y_aから排除情報

$C_2 = y_a{}^k \bmod p$

を計算し、特定端末番号ａと準備情報C_1と共に全端末に同報通信し、（３）前記議長端末は、共有鍵

$K = y^k \bmod p$

を求め、（４）前記各端末ｊ（$j \neq a$）は、$\Lambda = \{j, a\}$として、$\lambda(j, \Lambda)$と$\lambda(a, \Lambda)$を求め、前記準備情報C_1と前記排除情報C_2と自身の秘密情報S_jを用いて、

$C_1\hat{}(S_j \times \lambda(j, \Lambda) \bmod q) \times C_2\hat{}(\lambda(a, \Lambda) \bmod q) \bmod p$

を計算をすることにより、前記議長端末との共有鍵Ｋを求め、（ｉ）前記議長端末は、零でないＧＦ（ｑ）の元ｅを任意に生成し、前記共有鍵Ｋを用いて暗号化した暗号化ｅを全端末に同報通信し、（ii）前記議長端末は、新規元

$g' = g^{1/e \bmod q} \bmod p$

を求め、前記元ｇと置き換え、（iii）前記各端末ｊは、前記暗号化ｅを前記共有鍵Ｋを用いて復号化し、新規秘密情報

$S_j' = S_j \times e \bmod q$

（このとき、$(g')^{Sj'} \bmod p = (g)^{Sj} \bmod p$が成り立つ）を求める排他的鍵共有法であり、議長端末により公開鍵方式の秘密鍵を更新して排除端末を継続的に排除するという作用を有する。

【００２４】本発明の請求項５記載の発明は、相互に接続されたＮ台（Ｎは２以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をＳとし、前記Ｓおよび前記Ｎより大きい素数または素数のべき数をｐとし、（ｐ－１）の約数をｑとし、ＧＦ（ｐ）の元をｇとし、議長端末ｂが特定できる特定端末数を１とし、前記各端末ｉ（$1 \leqq i \leqq N$）は、

$S = \sum \lambda(i, \Lambda) \times S_i$（和は$i \in \Lambda$について行う）

（ただし、

$S_i = S + f_1 \times i \bmod q$（$f_1$は零でないＧＦ（ｑ）の元）、

$\lambda(i, \Lambda) = \prod \{L / (L - i)\}$（積は$L \in \Lambda - \{i\}$について行う）、

Λは、前記Ｎ台の端末の任意の２台からなる集合である）を満たす秘密情報S_iを秘密に保持しており、前記議長端末ｂは、全端末の公開鍵

$y = g^S \bmod p$

と、公開情報

$y_1 = g^{S1} \bmod p, y_2 = g^{S2} \bmod p, \cdots, y_N = g^{SN} \bmod p$

を利用でき、（１）前記議長端末ｂは、零でないＧＦ（ｑ）の元ｋを任意に生成し、準備情報

$C_1 = g^k \bmod p$

を計算し、（２）前記議長端末ｂは、特定端末ａの公開情報y_aから排除情報

$C_2=y_a{}^k \bmod p$
を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信し、(3)前記議長端末bは、共有鍵
$K=y^k \bmod p$
を求め、(4)前記各端末j(j≠a,b)は、$\Lambda=\{j,a\}$として、$\lambda(j,\Lambda)$と$\lambda(a,\Lambda)$を求め、前記準備情報C_1と前記排除情報C_2と自身の秘密情報S_jを用いて、
C_1^$(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2$^$(\lambda(a,\Lambda) \bmod q) \bmod p$
を計算をすることにより、共有鍵Kを求める排他的鍵共有法であり、端末のみからなるシステムにおいて固定的な議長端末のみに端末排除の権限を与えて、端末排除を可能とするという作用を有する。

【0025】本発明の請求項6記載の発明は、請求項5記載の排他的鍵共有法において、前記議長端末bを除く全ての端末は、前記議長端末bの公開情報
$y_b=g^{Sb} \bmod p$
を利用でき、前記議長端末bが、前記議長端末bの秘密情報S_bを用いて、全端末に配送する特定端末番号aと準備情報C_1と排除情報C_2に、ディジタル署名を付加し、前記各端末jが、前記議長端末の公開情報y_bを用いて、署名の検証を行うものであり、議長端末が配送する情報に署名して、議長端末の配送する情報を端末が検証して安全性を高めるという作用を有する。

【0026】本発明の請求項7記載の発明は、請求項3、4記載の排他的鍵共有法において、上記基地局または議長端末が、上記特定端末aに対して、上記元eを配送し、上記特定端末aは、新規秘密情報
$S_a'=S_a\times e \bmod q$
(このとき、(g')^$S_a' \bmod p=(g)$^$S_a \bmod p$が成り立つ)を求めるものであり、特定端末aにeを配送して秘密鍵を更新することで、排除した特定端末aを復帰させるという作用を有する。

【0027】本発明の請求項8記載の発明は、請求項1〜7記載の排他的鍵共有法において、前記乗法演算を、任意の有限体上の楕円曲線などの曲線上の加法演算に対応させるものであり、演算速度を高速化するという作用を有する。

【0028】以下、本発明の実施の形態について、図1〜図13を参照しながら詳細に説明する。

【0029】(第1の実施の形態)本発明の第1の実施の形態は、基地局と複数の端末からなる同報通信が可能な通信システムにおいて、基地局が、零でないGF(q)の元eを任意に生成して全端末に同報通信し、新規元$g'(=g^{1/e \bmod q} \bmod p)$を求めて、元gと置き換え、各端末iが、新規秘密情報$S_i'(=S_i\times e \bmod q)$を求める排他的鍵共有法である。

【0030】図1は、本発明の第1の実施の形態の排他的鍵共有法における通信システムの通常状態を示す図である。図1において、7は基地局、1〜6は、基地局の管理下にある端末である。同報通信網8は、無線などにより同報通信が可能な通信路である。図2は、本発明の第1の実施の形態の排他的鍵共有法における元gの更新方法を示す図である。図3は、本発明の第1の実施の形態の排他的鍵共有法における秘密鍵更新方法を示す図である。

【0031】図1〜図3を参照して、本発明の第1の実施の形態の排他的鍵共有法について説明する。図1に示すように、基地局7は、秘密鍵Sを作成して、秘密に保持する。秘密鍵Sより大きく、端末数6より大きな素数または素数のべきpを作成して、保持する。(p−1)の約数qを1つ求めて保持する。GF(q)の0でない元f_1を求めて保持する。

【0032】$f(z)=S+f_1\times z \bmod q$
を用いて、$S_i=f(i)$を計算することにより求めた秘密情報S_iを、各端末i(1≦i≦6)に暗号通信手段を用いて秘密に配送する。

【0033】6台の端末の任意の2台からなる集合をΛとしたとき、秘密情報S_iは、
$S=\sum\lambda(i,\Lambda)\times S_i$ (和はi∈Λについて行う)
$\lambda(i,\Lambda)=\prod\{L/(L-i)\}$ (積はL∈Λ−{i}について行う)
を満たす。ただし、集合Λ−{i}は、集合Λから集合{i}を除いた集合である。たとえば、Λ={1, 2}とすると、
$\lambda(1,\Lambda)=\prod\ \{L/(L-1)\}\ (L\in\{2\})$
$=2/(2-1)=2$
$\lambda(2,\Lambda)=\prod\ \{L/(L-2)\}\ (L\in\{1\})$
$=1/(1-2)=-1$
$\sum\lambda(i,\Lambda)\times S_i(i\in\Lambda)$
$=\lambda(1,\Lambda)\times S_1+\lambda(2,\Lambda)\times S_2$
$=2\times f(1)-f(2)$
$=2\cdot(S+f_1)-(S+2\cdot f_1)$
$=S$
となる。

【0034】各端末1,…,6は、秘密情報S_iを記憶部に保持する。基地局7は、法p、GF(p)の元gを記憶部に保持する。基地局7は、秘密情報$S_1,\dots,S_6$をそれぞれ指数とし、pを法とし、gを底とした公開情報$y_1(=g^{S1} \bmod p)$, $y_2(=g^{S2} \bmod p),\dots,y_6(=g^{S6} \bmod p)$を計算して記憶部に保持する。基地局7は、全端末1,…,6の秘密鍵Sを指数とし、pを法とし、gを底とする全端末の公開鍵$y(=g^S \bmod p)$を計算して記憶部に保持する。

【0035】端末5を排除する場合を説明する。基地局7は、GF(q)の0でない元kを任意に生成し、kを指数とし、pを法とし、gを底とする準備情報$C_1(=g^k \bmod p)$を計算する。整数kを指数、pを法とし、基地局7が特定した端末5の公開情報y_5を底とする排除情報

C_2（$=y_5{}^k$ modp）を計算する。kを指数、pを法、全端末1，…，6の公開鍵yを底とする共有鍵K（$=y^k$ modp$=g$^(S×k)modp）を求める。以上のC_1、C_2および特定端末番号5を全端末に同報通信する。

【0036】端末5を除いた全ての端末1，…，4，6で共有鍵を共有する場合の鍵共有フェーズを説明する。端末1では、自己の端末番号1と、受信した排除端末番号5から、Λ＝｛1，5｝として、

$\lambda(1,\Lambda)=5/(5-1)=5/4$

$\lambda(5,\Lambda)=1/(1-5)=-1/4$

を計算する。準備情報C_1(=g^k modp)と、排除情報C_2(=$y_5{}^k$ modp)を用いて、S_1とλ(1,Λ)を指数とし、C_1を底とするべき乗剰余値

C_1^(λ(1,Λ) modq) modp

と、λ(5,Λ)を指数とし、C_2を底とするべき乗剰余値

C_2^(λ(5,Λ) modq) modp

との積

C_1^(S_1×λ(1,Λ) modq)×C_2^(λ(5,Λ) modq) modp
＝g^(k×S_1×λ(1,Λ) modq)
×g^(k×S_5×λ(5,Λ) modq) modp
＝g^(k×(S_1×λ(1,Λ)＋S_5×λ(5,Λ) modq)) modp
＝g^(k×S modq) modp
＝K

を求めることによりKを得る。

【0037】以上の計算は、端末2～4，6でも同様に行うことができ、結果として、端末1～4，6で共通鍵Kを共有することができる。

【0038】一方、端末5においては、基地局7から同報通信された排除情報C_2(=$y_5{}^k$=g^(k×S_5) mod p)と、保持している情報から計算可能なべき乗剰余値(=$C_1{}^{S5}$ modp=g^(k×S_5) modp)が、同じであること、Λ＝｛5｝となってλ(5,Λ)が求められないことから、上記鍵共有フェーズでの共有鍵Kの算出ができない。

【0039】各端末は、

K＝g^(S×k) modp，
C_1＝g^k modp，
y＝g^S modp

から秘密鍵Sを求めることができないため、各分割秘密情報S_iは再利用できる。このため、次の鍵共有からはセットアップを行う必要はなく、準備フェーズと鍵共有フェーズを繰り返せばよい。

【0040】図2を参照して、基地局7が元gを更新する方法を説明する。基地局7は、零でないGF(q)の元e（乱数）を任意に生成し、eを全端末に同報通信する。基地局7は、新規元

g'＝$g^{1/e \bmod q}$ modp

を求め、元gと置き換える。

【0041】図3を参照して、端末が秘密鍵を更新する方法を説明する。各端末iは、新規秘密情報

S_i'＝S_i×e modq

を求めて保持する。このとき、

$(g')^{Si'}$ modp＝$(g)^{Si}$ modp

が成り立つ。

【0042】上記のように、本発明の第1の実施の形態では、排他的鍵共有法を、基地局が、零でないGF(q)の元eを任意に生成して全端末に同報通信し、新規元$g^{1/e \bmod q}$ modpを求めて、元gと置き換え、各端末iが、新規秘密情報S_i×e modqを求める構成としたので、少ない通信量と計算量で秘密鍵を更新できる。

【0043】（第2の実施の形態）本発明の第2の実施の形態は、相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、システム管理者が、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、新規元$g^{1/e \bmod q}$ modpを求め、管理する元gと置き換え、各端末iが、新規秘密情報S_i×e modqを求める排他的鍵共有法である。

【0044】図4は、本発明の第2の実施の形態の排他的鍵共有法における通常状態を示す図である。図4において、システム管理者9は、通信システムにアクセス可能な信頼できる機関であり、公開簿を作成して端末に提供する。図5は、本発明の第2の実施の形態の排他的鍵共有法における元gの更新方法を示す図である。図6は、本発明の第2の実施の形態の排他的鍵共有法における秘密鍵の更新方法を示す図である。

【0045】図4～図6を参照して、本発明の第2の実施の形態の排他的鍵共有法について説明する。図4に示すように、相互に接続された6台の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、Sおよび6より大きい素数または素数のべき数をpとし、(p－1)の約数をqとし、GF(p)の元をgとし、議長端末（任意の端末がなることができる）が特定できる特定端末数を1とする。

【0046】各端末i(1≦i≦6)は、

S＝Σλ(i，Λ)×S_i（和はi∈Λについて行う）

（ただし、

S_i＝S＋f_1×i modq（f_1は零でないGF(q)の元）、

λ(i，Λ)＝Π｛L／(L－i)｝(積はL∈Λ－｛i｝について行う)、

Λは、6台の端末の任意の2台からなる集合である）を満たす秘密情報S_iを秘密に保持する。システム管理者により管理された素数p，約数q，元gと、システム管

理者により管理された全端末の公開鍵

$y = g^S \bmod p$

と、システム管理者により管理された公開情報

$y_1 = g^{S1} \bmod p, y_2 = g^{S2} \bmod p, \cdots, y_6 = g^{S6} \bmod p$

を公開簿に載せて公開するので、各端末はこれらを利用できる。

【0047】議長端末は、零でないGF(q)の元kを任意に生成し、準備情報

$C_1 = g^k \bmod p$

を計算し、特定端末aの公開情報y_aから排除情報

$C_2 = y_a{}^k \bmod p$

を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信する。議長端末は、共有鍵

$K = y^k \bmod p$

を求める。

【0048】各端末j(j≠a)は、Λ={j,a}として、λ(j,Λ)とλ(a,Λ)を求め、準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、

C_1^(S_j×λ(j,Λ) mod q)×C_2^(λ(a,Λ) mod q) mod p

を計算をすることにより、議長端末との共有鍵Kを求める。

【0049】図5を参照して、元gの更新方法を説明する。システム管理者10は、零でないGF(q)の元e(乱数)を任意に生成し、eを全端末に同報通信する。システム管理者は、新規元

$g' = g^{1/e \bmod q} \bmod p$

を求め、管理する元gと置き換える。

【0050】図6を参照して、秘密鍵の更新方法を説明する。各端末iは、新規秘密情報

$S_i' = S_i \times e \bmod q$

を求めて保持する。このとき、$(g')^{Si'} \bmod p = (g)^{Si} \bmod p$が成り立つ。

【0051】上記のように、本発明の第2の実施の形態では、排他的鍵共有法を、システム管理者が、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、新規元$g^{1/e \bmod q} \bmod p$を求め、管理する元gと置き換え、各端末iが、新規秘密情報$S_i \times e \bmod q$を求める構成としたので、少ない通信量と計算量で秘密鍵を更新できる。

【0052】(第3の実施の形態)本発明の第3の実施の形態は、基地局と接続された6台の端末からなる同報通信が可能な通信システムにおいて、基地局で、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、新規元$g^{1/e \bmod q} \bmod p$を求め、元gと置き換え、各端末jが、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報$S_j \times e \bmod q$を求める排他的鍵共有法である。

【0053】図7は、本発明の第3の実施の形態の排他的鍵共有法を示す図である。図8は、本発明の第3の実施の形態の乱数配送方法を示す図である。図9は、端末を継続して排除する方法を説明する図である。

【0054】図7～図9を参照して、本発明の第3の実施の形態の排他的鍵共有法について説明する。図7に示すように、基地局7と、基地局7と接続された6台の端末からなる同報通信が可能な通信システムにおいて、秘密鍵をSとし、Sおよび6より大きい素数または素数のべき数をpとし、(p−1)の約数をqとし、基地局が特定できる端末数(以下、特定端末数という)を1とする。

【0055】各端末i(1≦i≦6)は、

S=Σλ(i,Λ)×S_i(和はi∈Λについて行う)

(ただし、

$S_i = S + f_1 \times i \bmod q$($f_1$は零でないGF(q)の元)、

λ(i,Λ)=Π{L/(L−i)}(積はL∈Λ−{i}について行う)、

Λは、6台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持している。

【0056】基地局は、$(S, p, g, S_1, \cdots, S_6)$を保持している。GF(p)の元をgとし、零でないGF(q)の元をkとしたとき、準備情報

$C_1 = g^k \bmod p$

を計算する。特定端末3の秘密情報S_3から排除情報

C_2=g^(k×S_3 mod q) mod p

を計算し、特定端末番号3と準備情報C_1と共に全端末に同報通信する。特定端末3を除く全ての端末j(j≠3)との共有鍵

K=g^(k×S mod q) mod p

を求める。

【0057】各端末j(j≠3)は、準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、S_jとλ(j,Λ)の法q上での積を指数とする、C_1のべき乗剰余値

C_1^(S_j×λ(j,Λ) mod q) mod p

と、法q上で求めたλ(3,Λ)を指数とする、C_2のべき乗剰余値

C_2^(λ(3,Λ) mod q) mod p

との積

C_1^(S_j×λ(j,Λ) mod q)×C_2^(λ(3,Λ) mod q) mod p

を計算をすることにより、基地局との共有鍵Kを求めて保持する。

【0058】図8を参照して、乱数eの配送方法を説明する。基地局7は、零でないGF(q)の元e(乱数)を任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信する。新規元

$g' = g^{1/e \bmod q} \bmod p$

を求め、元gと置き換える。

【0059】図9を参照して、継続排除の方法を説明する。各端末jは、暗号化eを共有鍵Kを用いて復号化

し、新規秘密情報

$S_j' = S_j \times e \mod q$

を求めて保持する。このとき、$(g')^{S_j'} \mod p = (g)^{S_j} \mod p$が成り立つ。

【0060】上記のように、本発明の第3の実施の形態では、排他的鍵共有法を、基地局で、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、新規元$g^{1/e \mod q} \mod p$を求め、元gと置き換え、各端末jが、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報$S_j \times e \mod q$を求める構成としたので、少ない通信量と計算量で秘密鍵を更新でき、継続して特定端末を排除できる。

【0061】(第4の実施の形態)本発明の第4の実施の形態は、相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、議長端末が、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、新規元$g^{1/e \mod q} \mod p$を求め、元gと置き換え、各端末jが、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報$S_j \times e \mod q$を求める排他的鍵共有法である。

【0062】図10は、本発明の第4の実施の形態の排他的鍵共有法を示す図である。図11は、本発明の第4の実施の形態の乱数配送方法を示す図である。図12は、端末を継続して排除する方法を示す図である。

【0063】図10～図12を参照して、本発明の第4の実施の形態の排他的鍵共有法について説明する。図10に示すように、相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、秘密鍵をSとし、Sおよび6より大きい素数または素数のべき数をpとし、(p−1)の約数をqとし、GF(p)の元をgとし、議長端末(任意の端末がなることができる。ここでは、端末6を議長端末とする)が特定できる特定端末数を1とする。

【0064】各端末i(1≦i≦6)は、

$S = \sum \lambda(i, \Lambda) \times S_i$(和は$i \in \Lambda$について行う)

(ただし、

$S_i = S + f_1 \times i \mod q$($f_1$は零でないGF(q)の元)、

$\lambda(i, \Lambda) = \prod \{L/(L-i)\}$(積は$L \in \Lambda - \{i\}$について行う)、

Λは、6台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持している。全端末の公開鍵

$y = g^S \mod p$

と、公開情報

$y_1 = g^{S1} \mod p, y_2 = g^{S2} \mod p, \cdots, y_6 = g^{S6} \mod p$

を公開簿に載せて公開するので、各端末はこれらを利用できる。

【0065】議長端末は、零でないGF(q)の元kを任意に生成し、準備情報

$C_1 = g^k \mod p$

を計算する。議長端末は、特定端末3の公開情報y_3から排除情報

$C_2 = y_3^k \mod p$

を計算し、特定端末番号3と準備情報C_1と共に全端末に同報通信する。議長端末は、共有鍵

$K = y^k \mod p$

を求める。

【0066】各端末j(j≠3)は、Λ={j, 3}として、λ(j, Λ)とλ(3, Λ)を求め、準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、

$C_1\text{^}(S_j \times \lambda(j, \Lambda) \mod q) \times C_2\text{^}(\lambda(3, \Lambda) \mod q) \mod p$

を計算をすることにより、議長端末との共有鍵Kを求める。

【0067】図11を参照して、乱数の配送方法を説明する。議長端末は、零でないGF(q)の元e(乱数)を任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信する。議長端末は、新規元

$g' = g^{1/e \mod q} \mod p$

を求め、元gと置き換える。

【0068】図12を参照して、継続排除の方法を説明する。各端末jは、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報

$S_j' = S_j \times e \mod q$

を求めて保持する。このとき、$(g')^{S_j'} \mod p = (g)^{S_j} \mod p$が成り立つ。

【0069】上記のように、本発明の第4の実施の形態では、排他的鍵共有法を、議長端末が、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、新規元$g^{1/e \mod q} \mod p$を求め、元gと置き換え、各端末jが、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報$S_j \times e \mod q$を求める構成としたので、少ない通信量と計算量で秘密鍵を更新でき、継続して特定端末を排除できる。

【0070】なお、継続排除した端末を復帰させるために、新たに秘密鍵と公開鍵のペアを作成する必要があり、以前の公開鍵が使用できないが、新たに秘密鍵と公開鍵のペアを作成することなく、継続排除した端末を復帰させることができる。そのためには、次のようにすればよい。

【0071】基地局または議長端末が、特定端末3に対して、元eを配送し、特定端末3は、新規秘密情報

$S_3' = S_3 \times e \mod q$

(このとき、$(g')\text{^}S_3' \mod p = (g)\text{^}S_3 \mod p$が成り立つ)

を求める。このようにして、秘密鍵と公開鍵のペアを新たに作成しないで、以前の公開鍵をそのまま使用することができる。特定端末が複数あり、そのうちのいくつかのみ復帰させる場合には、復帰させたい端末のみに秘密

にeを配送すればよい。

【0072】（第5の実施の形態）本発明の第5の実施の形態は、相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、議長端末が、零でないGF(q)の元kを任意に生成し、準備情報C_1を計算し、特定端末aの公開情報y_aから排除情報C_2を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信し、共有鍵Kを求め、各端末は準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、共有鍵Kを求める排他的鍵共有法である。

【0073】図13は、本発明の第5の実施の形態の排他的鍵共有法を示す図である。図13を参照して、本発明の第5の実施の形態の鍵共有方法について説明する。相互に接続された6台の端末からなる同報通信が可能な通信システムにおいて、秘密鍵をSとし、Sおよび6より大きい素数または素数のべき数をpとし、(p−1)の約数をqとし、GF(p)の元をgとし、議長端末2が特定できる特定端末数を1とする。

【0074】各端末i(1≦i≦6)は、

$S=\sum\lambda(i,\Lambda)\times S_i$（和は$i\in\Lambda$について行う）

（ただし、

$S_i=S+f_1\times i \bmod q$（$f_1$は零でないGF(q)の元）、

$\lambda(i,\Lambda)=\prod\{L/(L-i)\}$（積は$L\in\Lambda-\{i\}$について行う）、

Λは、6台の端末の任意の2台からなる集合である）を満たす秘密情報S_iを秘密に保持している。議長端末2は、全端末の公開鍵

$y=g^S \bmod p$

と、公開情報

$y_1=g^{S1} \bmod p, y_2=g^{S2} \bmod p,\cdots,y_6=g^{S6} \bmod p$

を公開簿に載せて公開するので、各端末はこれらを利用できる。

【0075】議長端末2は、零でないGF(q)の元kを任意に生成し、準備情報

$C_1=g^k \bmod p$

を計算する。特定端末aの公開情報y_aから排除情報

$C_2=y_a{}^k \bmod p$

を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信する。共有鍵

$K=y^k \bmod p$

を求める。

【0076】各端末j(j≠a,b)は、Λ={j,a}として、λ(j,Λ)とλ(a,Λ)を求め、準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、

$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$

を計算をすることにより、共有鍵Kを求める。

【0077】なお、議長端末を除く全ての端末が、議長端末の公開情報

$y_b=g^{Sb} \bmod p$

を利用できるようにし、議長端末が、議長端末の秘密情報S_bを用いて、全端末に配送する特定端末番号aと準備情報C_1と排除情報C_2に、ディジタル署名を付加することにより、各端末jが、議長端末の公開情報y_bを用いて、署名の検証を行うことができる。

【0078】上記のように、本発明の第5の実施の形態では、排他的鍵共有法を、議長端末が、零でないGF(q)の元kを任意に生成し、準備情報C_1を計算し、特定端末aの公開情報y_aから排除情報C_2を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信し、共有鍵Kを求め、各端末は準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、共有鍵Kを求める構成としたので、議長端末を固定して特定端末を排除できる。

【0079】なお、基地局または議長端末が、特定端末aに対して、元eを配送し、特定端末aが、新規秘密情報

$S_a'=S_a\times e \bmod q$

（このとき、$(g')\hat{}S_a' \bmod p=(g)\hat{}S_a \bmod p$が成り立つ）を求めることにより、排除した端末を復帰させることができる。

【0080】また、乗法演算を、任意の有限体上の楕円曲線などの曲線上の加法演算に対応させることで、高速に演算することができる。

【0081】

【発明の効果】以上説明したように、本発明では、基地局と、基地局と接続されたN台（Nは2以上の整数）の端末からなる同報通信が可能な通信システムの排他的鍵共有法を、秘密鍵をSとし、SおよびNより大きい素数または素数のべき数をpとし、(p−1)の約数をqとし、基地局が特定できる端末数（以下、特定端末数という）を1とし、各端末i(1≦i≦N)は、

$S=\sum\lambda(i,\Lambda)\times S_i$（和は$i\in\Lambda$について行う）

（ただし、

$S_i=S+f_1\times i \bmod q$（$f_1$は零でないGF(q)の元）、

$\lambda(i,\Lambda)=\prod\{L/(L-i)\}$（積は$L\in\Lambda-\{i\}$について行う）、

Λは、N台の端末の任意の2台からなる集合である）を満たす秘密情報S_iを秘密に保持しており、基地局は、$(S,p,g,S_1,\cdots,S_N)$を保持し、（1）基地局は、GF(p)の元をgとし、零でないGF(q)の元をkとしたとき、準備情報

$C_1=g^k \bmod p$

を計算し、（2）基地局は、特定端末aの秘密情報S_aから排除情報

$C_2=g\hat{}(k\times S_a \bmod q) \bmod p$

を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信し、（3）基地局は、特定端末aを除く全ての端末j(j≠a)との共有鍵

$K=g\hat{}(k\times S \bmod q) \bmod p$
を求め、(4)各端末j(j≠a)は、準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、S_jと$\lambda(j,\Lambda)$の法q上での積を指数とする、C_1のべき乗剰余値
$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q) \bmod p$
と、法q上で求めた$\lambda(a,\Lambda)$を指数とする、C_2のべき乗剰余値
$C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$
との積
$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$
を計算をすることにより、基地局との共有鍵Kを求め、(i)基地局は、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、(ii)基地局は、新規元
$g'=g^{1/e \bmod q} \bmod p$
を求め、元gと置き換え、(iii)各端末iは、新規秘密情報
$S_i'=S_i\times e \bmod q$
(このとき、$(g')^{S_i'} \bmod p=(g)^{S_i} \bmod p$が成り立つ)を求める構成としたので、基地局の通信量がeのみと少なく、システムパラメータ元g以外の公開情報が変更されないので、高速に秘密情報の更新ができるという効果が得られる。

【0082】また、相互に接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i)システム管理者は、零でないGF(q)の元eを任意に生成し、eを全端末に同報通信し、(ii)システム管理者は、新規元
$g'=g^{1/e \bmod q} \bmod p$
を求め、管理する元gと置き換え、(iii)各端末iは、新規秘密情報
$S_i'=S_i\times e \bmod q$
を求める構成としたので、システム管理者の通信量がeのみと少なく、システムパラメータ元g以外の公開情報が変更されないので、高速に秘密情報の更新ができるという効果が得られる。

【0083】また、基地局と、基地局と接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i)基地局は、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、(ii)基地局は、新規元
$g'=g^{1/e \bmod q} \bmod p$
を求め、元gと置き換え、(iii)各端末jは、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報
$S_j'=S_j\times e \bmod q$
を求める構成としたので、排他的鍵共有で共有した共有鍵を用いて配送した乱数を用いて端末の秘密情報を更新して、以降の排他的鍵共有で排除した端末が復帰できないようにできるという効果が得られる。

【0084】また、相互に接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、(i)議長端末は、零でないGF(q)の元eを任意に生成し、共有鍵Kを用いて暗号化した暗号化eを全端末に同報通信し、(ii)議長端末は、新規元
$g'=g^{1/e \bmod q} \bmod p$
を求め、元gと置き換え、(iii)各端末jは、暗号化eを共有鍵Kを用いて復号化し、新規秘密情報
$S_j'=S_j\times e \bmod q$
を求める構成としたので、排他的鍵共有で共有した共有鍵を用いて配送した乱数を用いて端末の秘密情報を更新して、以降の排他的鍵共有で排除した端末が復帰できないようにできるという効果が得られる。

【0085】また、相互に接続されたN台(Nは2以上の整数)の端末からなる同報通信が可能な通信システムの排他的鍵共有法において、秘密鍵をSとし、SおよびNより大きい素数または素数のべき数をpとし、(p−1)の約数をqとし、GF(p)の元をgとし、議長端末bが特定できる特定端末数を1とし、各端末i(1≦i≦N)は、
$S=\sum\lambda(i,\Lambda)\times S_i$ (和はi∈Λについて行う)
(ただし、
$S_i=S+f_1\times i \bmod q$ (f_1は零でないGF(q)の元)、
$\lambda(i,\Lambda)=\prod\{L/(L-i)\}$ (積はL∈Λ−{i}について行う)、
Λは、N台の端末の任意の2台からなる集合である)を満たす秘密情報S_iを秘密に保持しており、議長端末bは、全端末の公開鍵
$y=g^S \bmod p$
と、公開情報
$y_1=g^{S1} \bmod p, y_2=g^{S2} \bmod p,\cdots, y_N=g^{SN} \bmod p$
を利用でき、(1)議長端末bは、零でないGF(q)の元kを任意に生成し、準備情報
$C_1=g^k \bmod p$
を計算し、(2)議長端末bは、特定端末aの公開情報y_aから排除情報
$C_2=y_a{}^k \bmod p$
を計算し、特定端末番号aと準備情報C_1と共に全端末に同報通信し、(3)議長端末bは、共有鍵
$K=y^k \bmod p$
を求め、(4)各端末j(j≠a,b)は、Λ={j,a}として、$\lambda(j,\Lambda)$と$\lambda(a,\Lambda)$を求め、準備情報C_1と排除情報C_2と自身の秘密情報S_jを用いて、
$C_1\hat{}(S_j\times\lambda(j,\Lambda) \bmod q)\times C_2\hat{}(\lambda(a,\Lambda) \bmod q) \bmod p$
を計算をすることにより、共有鍵Kを求める構成としたので、議長端末以外の端末は他の端末の公開情報を保持する必要が無く、議長端末のみが他の端末の公開情報を

利用できるので他の端末は議長端末になれないという効果が得られる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態の鍵共有方法における通常状態を示す図、

【図2】第1の実施の形態の鍵共有方法における元ｇの更新方法を示す図、

【図3】第1の実施の形態の鍵共有方法において秘密鍵の更新方法を示す図、

【図4】本発明の第2の実施の形態の鍵共有方法における通常状態を示す図、

【図5】第2の実施の形態の鍵共有方法における元ｇの更新方法を示す図、

【図6】第2の実施の形態の鍵共有方法において秘密鍵の更新方法を示す図、

【図7】本発明の第3の実施の形態の鍵共有方法における端末3の排除状態を示す図、

【図8】第3の実施の形態の鍵共有方法における乱数配送方法を示す図、

【図9】第3の実施の形態の鍵共有方法における端末の継続排除の方法を示す図、

【図10】本発明の第4の実施の形態の鍵共有方法における端末3の排除状態を示す図、

【図11】第4の実施の形態の鍵共有方法における乱数配送方法を示す図、

【図12】第4の実施の形態の鍵共有方法における端末の継続排除の方法を示す図、

【図13】本発明の第5の実施の形態の鍵共有方法における議長端末の固定方法を示す図である。

【符号の説明】

1〜6　端末1〜端末6

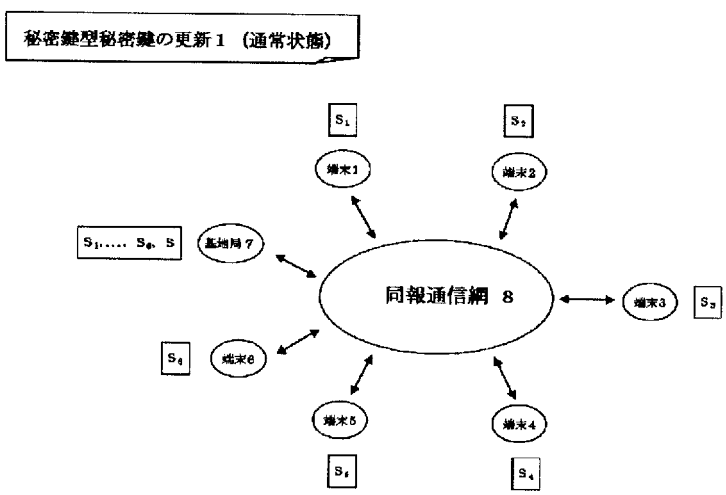
7　基地局

8　同報通信網

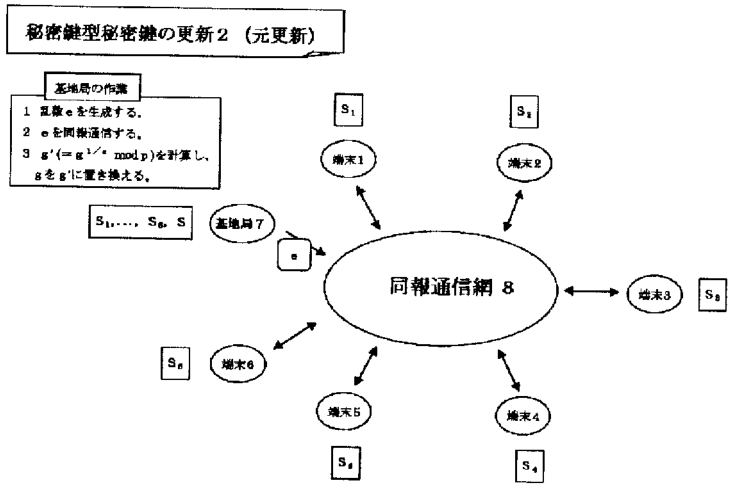
9　システム管理者

10　議長端末

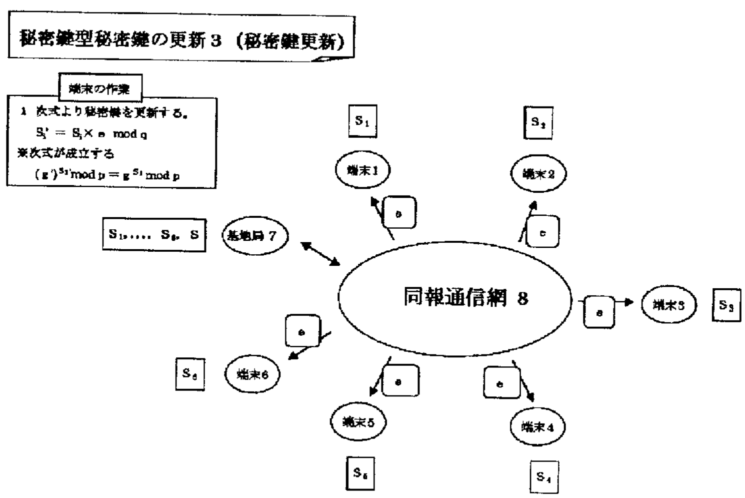
【図1】



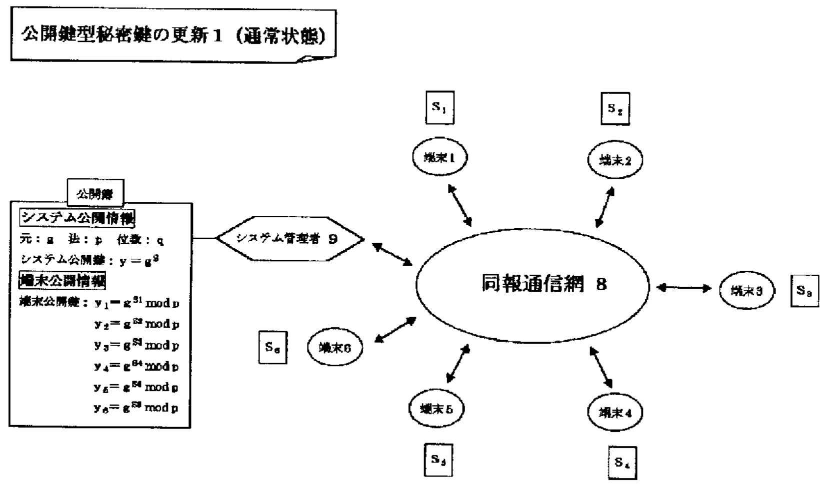
【図2】


秘密鍵型秘密鍵の更新2 (元更新)
基地局の作業
1 乱数eを生成する。
2 eを同報通信する。
3 g'(=g^{1/e} mod p)を計算し、gをg'に置き換える。
S1,…, S6, S
基地局7
e
同報通信網 8
端末1
S1
端末2
S2
端末3
S3
端末4
S4
端末5
S5
端末6
S6

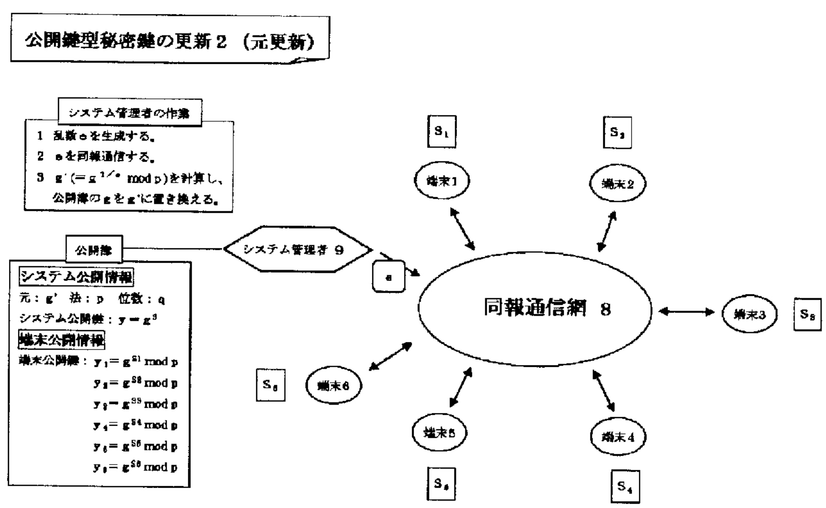
【図3】


秘密鍵型秘密鍵の更新3 (秘密鍵更新)
端末の作業
1 次式より秘密鍵を更新する。
Si' = Si × e mod q
※次式が成立する
(g')^{Si'} mod p = g^{Si} mod p
S1,…, S6, S
基地局7
同報通信網 8
e
端末1
S1
端末2
S2
端末3
S3
端末4
S4
端末5
S5
端末6
S6

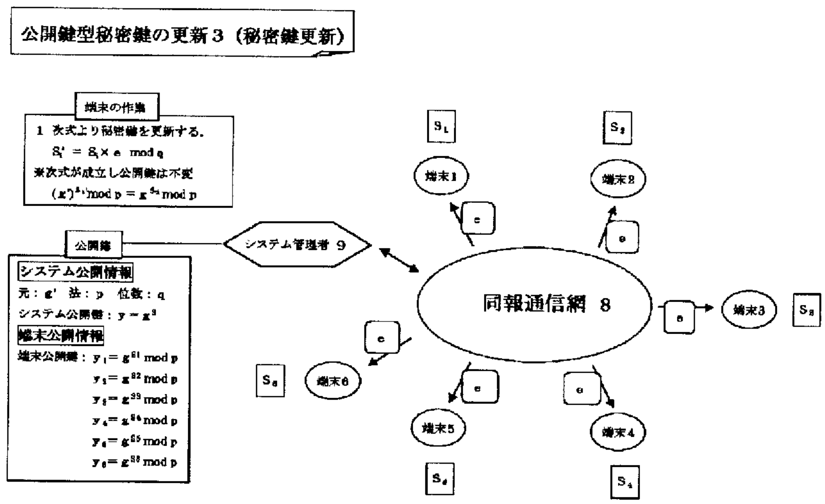
【図4】


公開鍵型秘密鍵の更新1（通常状態）
公開簿
システム公開情報
元：g　法：p　位数：q
システム公開鍵：y = g^S
端末公開情報
端末公開鍵：y1 = g^S1 mod p
y2 = g^S2 mod p
y3 = g^S3 mod p
y4 = g^S4 mod p
y5 = g^S5 mod p
y6 = g^S6 mod p
システム管理者 9
同報通信網 8
端末1
端末2
端末3
端末4
端末5
端末6
S1
S2
S3
S4
S5
S6

【図5】

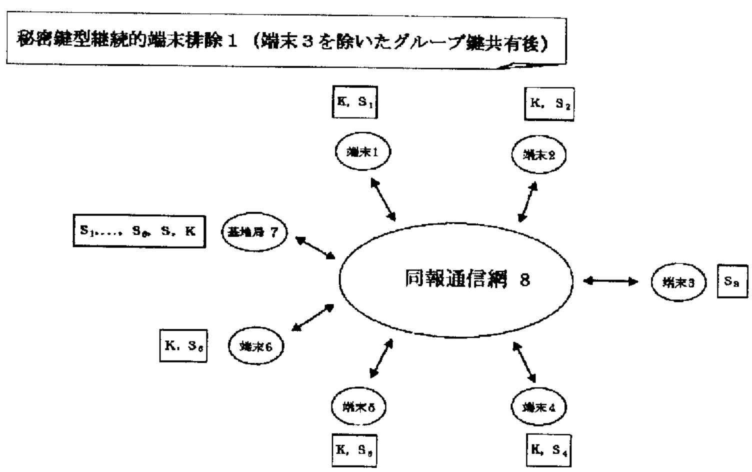

公開鍵型秘密鍵の更新2（元更新）
システム管理者の作業
1 乱数eを生成する。
2 eを同報通信する。
3 g'(=g^{1/e} mod p)を計算し、公開簿のgをg'に置き換える。
公開簿
システム公開情報
元：g'　法：p　位数：q
システム公開鍵：y = g^S
端末公開情報
端末公開鍵：y1 = g^S1 mod p
y2 = g^S2 mod p
y3 = g^S3 mod p
y4 = g^S4 mod p
y5 = g^S5 mod p
y6 = g^S6 mod p
システム管理者 9
e
同報通信網 8
端末1
端末2
端末3
端末4
端末5
端末6
S1
S2
S3
S4
S5
S6

【図6】



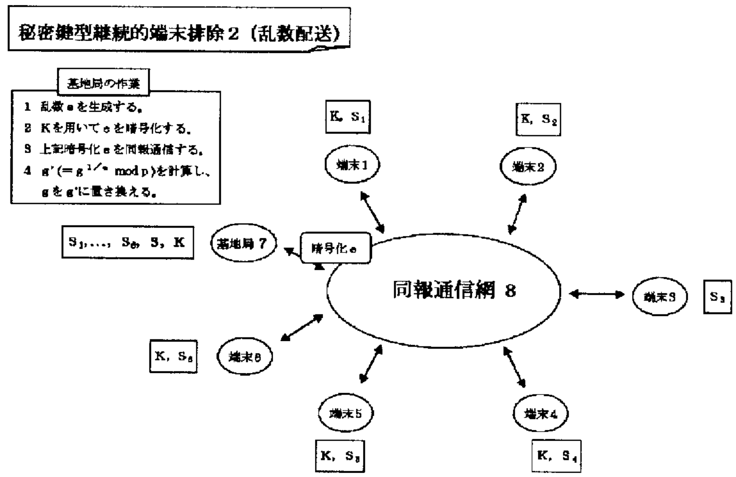
公開鍵型秘密鍵の更新3（秘密鍵更新）
端末の作業
1 次式より秘密鍵を更新する。
$S_i' = S_i \times e \mod q$
※次式が成立し公開鍵は不変
$(g')^{S_i'} \mod p = g^{S_i} \mod p$
公開簿
システム公開情報
元：g' 法：p 位数：q
システム公開鍵：$y = g^S$
端末公開情報
端末公開鍵：$y_1 = g^{S1} \mod p$
$y_2 = g^{S2} \mod p$
$y_3 = g^{S3} \mod p$
$y_4 = g^{S4} \mod p$
$y_5 = g^{S5} \mod p$
$y_6 = g^{S6} \mod p$
システム管理者 9
同報通信網 8
端末1
端末2
端末3
端末4
端末5
端末6
S_1
S_2
S_3
S_4
S_5
S_6
e

【図7】

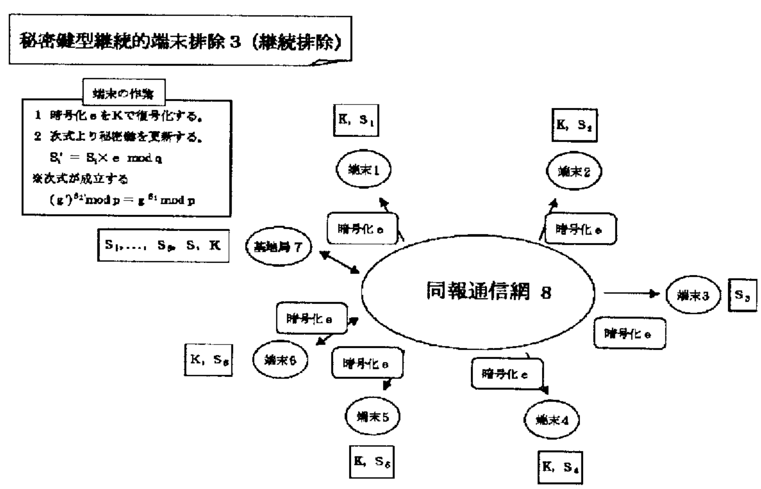


秘密鍵型継続的端末排除1（端末3を除いたグループ鍵共有後）
基地局 7
$S_1, \ldots, S_6, S, K$
同報通信網 8
端末1
端末2
端末3
端末4
端末5
端末6
K, S_1
K, S_2
S_3
K, S_4
K, S_5
K, S_6

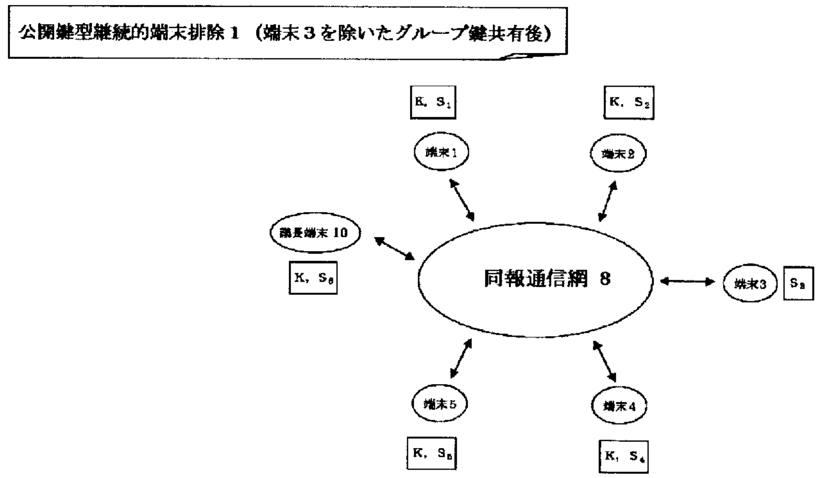
【図8】


秘密鍵型継続的端末排除２（乱数配送）
基地局の作業
1 乱数eを生成する。
2 Kを用いてeを暗号化する。
3 上記暗号化eを同報通信する。
4 g'(=g^{1/e} mod p)を計算し、
gをg'に置き換える。
K, S1
端末1
K, S2
端末2
S1,…, S6, S, K
基地局７
暗号化e
同報通信網 8
端末3
S3
K, S6
端末6
端末5
K, S5
端末4
K, S4

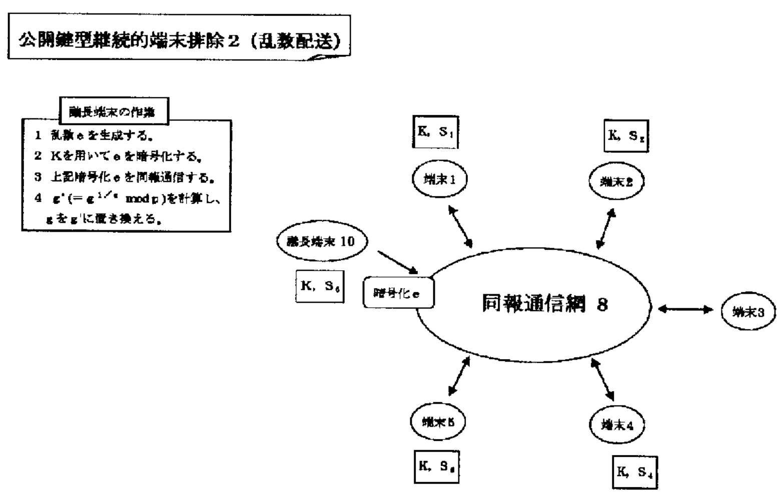
【図9】


秘密鍵型継続的端末排除３（継続排除）
端末の作業
1 暗号化eをKで復号化する。
2 次式上り秘密鍵を更新する。
Si' = Si × e mod q
※次式が成立する
(g')^{Si'} mod p = g^{Si} mod p
K, S1
端末1
K, S2
端末2
暗号化e
暗号化e
S1,…, S6, S, K
基地局７
同報通信網 8
端末3
S3
暗号化e
暗号化e
K, S6
端末6
暗号化e
暗号化e
端末5
K, S5
端末4
K, S4

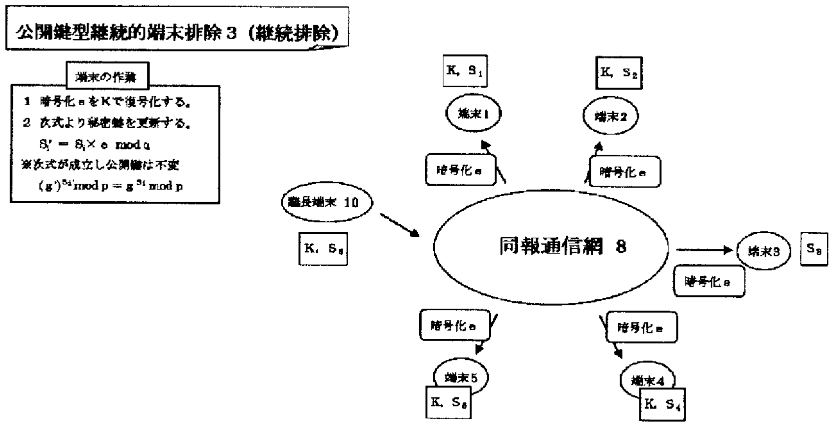
【図10】


公開鍵型継続的端末排除1（端末3を除いたグループ鍵共有後）
K, S_1
K, S_2
端末1
端末2
議長端末 10
K, S_6
同報通信網 8
端末3
S_3
端末5
端末4
K, S_5
K, S_4

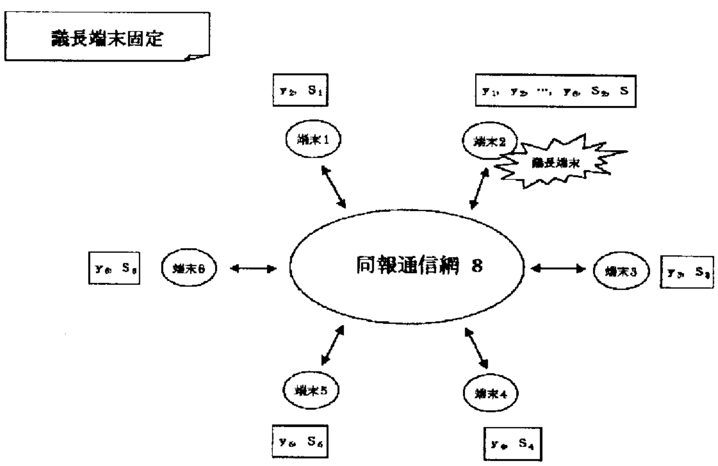
【図11】


公開鍵型継続的端末排除2（乱数配送）
議長端末の作業
1 乱数eを生成する。
2 Kを用いてeを暗号化する。
3 上記暗号化eを同報通信する。
4 $g'(=g^{1/e} \bmod p)$を計算し、
gをg'に置き換える。
K, S_1
K, S_2
端末1
端末2
議長端末 10
K, S_6
暗号化e
同報通信網 8
端末3
端末5
端末4
K, S_5
K, S_4

【図12】



【図13】



フロントページの続き

(72)発明者　松崎　なつめ
神奈川県横浜市港北区新横浜三丁目20番地
８　株式会社高度移動通信セキュリティ技
術研究所内

(72)発明者　松本　勉
神奈川県横浜市青葉区柿の木台13－45

Ｆターム(参考)　5J104 AA16 AA22 EA01 EA04 EA19
EA28 EA30 MA06 NA16 NA18
PA01 PA04 PA05
5K067 AA34 EE22 HH36